

OFFICE OF CONGRESSIONAL AFFAIRS

Routing Slip

	ACTION	INFO
1. D/OCA		x
2. DD/Legislation		x
3. DD/Senate Affairs	x	
4. DD/House Affairs		x
5. Admin Officer		
6. Executive Officer		x
7. FOIA Officer		
8. Constituent Inquiries Officer		
9.		
10.		
11.		
12.		

SUSPENSE

DATE

Action Officer:

Remarks: DCI; DDCI-Designate; OGC
NIO/FDIA(Hutchinson); DO/CI
PAO, Registry

Name/Date

STAT
STAT
STAT

SSCI
 OCA FILE
 Record
 RECPT #

Dave Durenberger news

U.S. Senator for Minnesota



FOR IMMEDIATE RELEASE
 Issued: April 4, 1986

Contact: Karen Doyne
 (202) 224-9475

CONGRESSIONAL AFFAIRS

86-1159

**The Year of the Leak
 Classified Information and the News Media
 Remarks by Senator Dave Durenberger
 Chairman, Senate Select Committee on Intelligence
 Chicago Council on Foreign Relations
 Chicago, Illinois
 April 4, 1986**

The press has called 1985 the "Year of the Spy" and in many ways it was.

But, while recent headlines have been filled with names like Walker and Howard and Chin and Pelton, the nation's readers are also being bombarded with headlines like:

"U.S. discloses secret plan by the Sandinistas"

"CIA anti-Quaddafi plan backed"

"Secret U.S. missile aid reported"

These and dozens of other stories about sensitive matters involving intelligence and national security are based on deliberate leaks.

This kind of unauthorized disclosure of highly classified information -- especially the deliberate leaking of intelligence information that compromises sensitive sources and methods -- is sapping the strength of our national leaders. It is hurting our credibility with our allies. It is unnecessarily complicating relations with our adversaries. And, it is harming the morale and effectiveness of the dedicated men and women in our own intelligence agencies.

At a hearing of the Senate Intelligence Committee last fall on counter-intelligence and security problems, CIA Director Bill Casey stated that leaks "do more damage than anything else" to our intelligence capabilities and to "our reputation and reliability" in dealing with other nations.

I share Director Casey's concern. He is frustrated. The president is frustrated. And, our committee is deeply upset because the executive tends to lay blame on the elected members of the federal government and those individuals in the executive branch who oppose thorough congressional oversight of national security matters do so consistently.

A good many commentators and some government officials have criticized members of the Intelligence Committee for talking publicly about intelligence problems, even when we say nothing that is classified. And, of course, we've taken blame for the leaking of classified information, as well.

-2-

But, the facts are that there is probably nowhere else in Washington -- in the Congress or the administration -- where public officials are more concerned about protecting secrets and resisting the temptations to discuss classified matters in public than the Senate Select Committee on Intelligence.

Those who malign the committee for overt or covert release of classified information are, more often than not, seeking to destroy the credibility of the oversight process, rather than to improve security.

Every administration has faced the problem of leaks, but none so much as this one.

Some disclosures, of course, may be inadvertent. Recently, in reply to a question about aiding anti-communist rebels in Angola, the president said, and I quote, "We all believe that a covert operation would be more useful to us and have more chance of success right now than the overt proposal that has been made in the Congress."

The same thing occurred back in 1983, when the president first called publicly for Congress to support the "Freedom Fighters" in Nicaragua -- covertly. Some critics have charged that the phrase "Senate Intelligence" is an oxymoron; I would make the same assertion with respect to publicly-discussed "covert" aid.

So, what is the scope of the problem of leaking sensitive intelligence and national security information? How serious a situation are we really talking about?

Let me give you two quick examples:

In recent months, the press has reported alleged CIA covert action against Libyan Dictator Moammar Quaddafi. Whether true or false, such reports can lead to increased Libyan terrorism against Americans and U.S. interests.

And, of course, the recent moves by executive branch officials to release sensitive intelligence on Nicaraguan lobbying efforts on the contra aid issue were a classic example of ignoring the need to protect intelligence sources and methods.

A forceful press release from our committee gave the White House second thoughts about formally releasing the material. But, the Washington Times ran a leaked story on a "mole" in high Sandinista places and within two weeks three Nicaraguan officials were arrested and charged as CIA assets.

These two examples of dangerous leaks are only the latest in a long series of unauthorized disclosures that have jeopardized intelligence sources and methods.

During the SALT II debate in the late 1970s, leaks and disclosures about possible Soviet arms control violations, and our technical collection capabilities, gave the Soviets tremendous insight into our collection efforts, insight that can result in countermeasures to deny us vital strategic intelligence.

The same things happens when arms control compliance issues are leaked before the president can use the Standing Consultative Commission to attempt to find a solution through quiet diplomacy. On several occasions these issues have been leaked before or during SCC discussions making it that much harder for the Soviets to back down.

-3-

Since the Reagan Administration took office, and the Senate became Republican, overt use of top secret information on Soviet treaty compliance has increased substantially.

On November 6, 1985, for example, the Washington Post published a column by Rowland Evans and Robert Novak revealing what they claimed was a key finding in a national intelligence estimate on arms control monitoring. The article cited alleged difficulties in monitoring compliance. That disclosure clearly served the interest of one side in the debate within the administration over policy for arms control negotiations in preparation for the Reagan-Gorbachev summit. Their source clearly sought such advantage and was willing to use a calculated leak of sensitive intelligence information to obtain it. The frequency with which columns by these two writers are peppered with sensitive national security information has led to the rumor in Washington that the administration has two hot-lines -- one to the Kremlin and the other to Evans and Novak.

There are legitimate differences of opinion in this country about the wisdom of engaging in arms control negotiations with the Soviets; and verification of compliance with arms control treaties is at the heart of those differences. But, the overt use of leaks to discredit the verification process has no legitimate place in this crucial national debate.

Leaks are of particular concern in a crisis situation where the deployment of counter-terrorism rescue forces is disclosed. Such disclosures can doom a rescue effort before it gets off the ground. Network news directors have recently been pressed to withhold just his kind of information which they've obtained while the same information has been totally withheld from the Congress.

The cumulative impact of this misuse of leaks is to inhibit national leaders from taking measures that require secrecy for their success. That is a terrible and intolerable outcome. An unwillingness to take risks could prove fatal in a future crisis.

The most frequently mentioned "solution" to the leak problem, of course, is to shut down the flow of classified information to policymakers. The best reason for not plugging leaks in this manner, however, is that it will not work in the system we have today. Moreover, it is certainly not desirable. Failure to share information with the proper officials results in the loss of valuable advice and consultation.

So the answer to leaks is not closing down the legitimate flow of information to policy makers. It is in doing something about the underlying attitudes that foster disrespect of the rules of secrecy.

The current ethos in Washington, of course, is just the opposite.

When the White House offers to release classified intelligence reports in order to sway votes in Congress, the lack of concern for sources and methods sends just the wrong message to subordinates in the administration: namely, "You, too, may play fast and loose with security."

When the executive branch officials then purport to discuss the intelligence sources themselves, we can only conclude that the message of laxity at the highest levels has been received by those further down.

-4-

What is needed today, throughout the government, is a new dedication to the ethic of silence by those entrusted with the most sensitive national secrets.

That ethic is not easily adhered to. It often requires sacrificing one's own ends or those of one's office or particular ideology, in order to serve larger national interests.

Frequently, the personal interest behind leaks lies in the protecting the position of one's own boss, or publicizing one's own opinions through the media. But, to use one's office and access to trusted national secrets in this manner is narcissism on the worst order.

Unfortunately, the news media must share at least part of the blame for this kind of prostitution of national secrets. Generally, the news media are all too willing to be used in return for information, particularly in the case of columnists who share a common ideology with those who are attempting to use classified information for their own selfish ends.

Also aggravating the problem is a woeful lack of knowledge on the part of some policymakers who regularly handle sensitive intelligence information.

Few senior officials appear to understand fully the damage that can result from disclosures of intelligence which does not appear sensitive on the surface, despite its high classification.

This inattention to the importance of maintaining security is not entirely the fault of officials who have not been fully briefed on the actual sensitivity of the information they get. Fortunately, in practice, the most sensitive information received by members of Congress is handled only by the Intelligence Committees, whose members have been fully briefed on why secrecy is necessary.

The fact that leakers are seldom caught and even less often punished -- regardless of the seriousness of the violation of trust -- also contributes to the problem. A security system based on the marginally deterrent effect of fruitless investigations is not likely to overcome the strong incentives that fuel the engines of bureaucratic conflict through the use of leaks.

Those who are at the greatest disadvantage in the leaking game are the critics outside of government.

In the debate over the president's strategic defense initiative, a physicist at Livermore, Ray Kidder, was quoted in the Los Angeles Times as saying: "The public is getting swindled by one side that has access to classified information and can say whatever it wants and not go to jail, whereas we -- we the skeptics -- can't say whatever we want. We would go to jail. That's the difference."

Another factor contributing to the growing problem of leaks is the large number of intelligence experts outside government -- many of whom are alumni of the intelligence community -- who comment to the press on "methods" even if, legally, they are barred from discussing "sources".

These individuals can carry with them important national security information and sometimes even a motive to engage in leaks -- without the threat of a supervisor or loss of employment hanging over them.

-5-

When the press is filled with public announcements of arrests, disclosures from executive branch sources, and comments by former intelligence officials, the congressional oversight committees are placed in an awkward and difficult position.

Because we are visible -- and because we are politicians -- it is often assumed that we are able and willing to provide confirmation or denial of information which has been leaked. A response of "no comment" simply makes oversight look passive and ineffective. In the long run, oversight committees with that kind of image can do little to help maintain broad support for legitimate intelligence programs.

If the executive branch would make some comment on the record in these situations, there would be no need for any further statement by the oversight committee.

The best procedure for handling problems caused by leaks is not to pretend they will go away, but to respond publicly. Nothing kills public attention quicker than satisfying the intense, but temporary, appetite for information.

Over the long haul, however, the single most important element in changing the environment for leaks is strong leadership that demonstrates, by example as well as rhetoric, a commitment to security.

Leaders who are willing to forego the game of one-upmanship -- and avoid the temptation to seek short-term personal gain at the expense of the larger national interest -- will take the first essential step toward stopping the use of leaks as an accepted political tactic.

Along with that kind of commitment, the administration and Congress must now look at specific administrative and legislative actions to enhance security for sensitive information.

As an initial step, the Senate Intelligence Committee is currently engaged in consultation with the NSC staff and other key officials in an attempt to reach agreement with the administration on an agenda for action to strengthen security for the most sensitive information. There are at least eight important items on that agenda.

The first item sure to be on our list is the need to educate policy makers on the damage caused by leaks.

Tailored security briefings by the intelligence community should be given to every new member of the White House and National Security Council staffs who handles intelligence information, as well as to political appointees in various agencies and to members of Congress and their staffs who have access to such information.

Secondly, in the context of the Intelligence Committee's larger agenda, we are also prepared to consider a proposal to deal with criminal penalties for leaks of highly classified information.

The committee's primary concern in considering the imposition of criminal penalties is the compromise of vital intelligence source and methods. But, at the same time, the law must provide room for public discussion of intelligence community failures. We should not withhold information which exposes failures or mistakes if that information does not endanger the continued effectiveness of the intelligence community or its vital sources and methods.

-6-

Third, any attempt to curb leaks must realize that the current classification and declassification process is at the heart of the problem.

I believe the time has come when the Congress and the executive branch must begin a serious dialogue on whether new legislation is necessary or desirable to protect the integrity of national secrets.

New legislation should be the last resort, however, after administrative measures are implemented. After all, the classification system is product of the executive branch. Information is labeled "confidential," "secret," or "top secret" -- and sometimes also placed in various special access compartments -- on the basis of standards set by the president in an executive order.

Even when Congress has legislated penalties for disclosure of specific categories of information, the executive branch of information, the executive branch determines how the information is classified and the procedures for authorized disclosure.

The only exception -- never used as yet -- is a provision in the resolution creating the Senate Intelligence Committee which prescribes a procedure for the full Senate to decide, in closed session, that classified information should be release over the president's objections.

One dimension of the classification problem is overclassification and unnecessary classification, which discredits the whole system and dissipates the resources available for the protection of truly sensitive secrets. Any effort to deter leaks must include a systematic attack on excessive classification.

The Senate Intelligence Committee's recommendations on information security state that recent espionage cases "have enlightened the security problems that result in large measure from attempting to protect too much and thereby stretching personnel and other security programs too thin." The last Justice Potter Stewart called this problem "secrecy for its own sake," in his opinion in the 1972 Pentagon Papers Case.

In its recommendations, the Intelligence Committee has recommended more extensive reform of the classification system than the executive branch has been willing to consider.

While the initiatives developed by the administration thus far are commendable and should be implemented at once, our committee proposes streamlining the system by adopting a simple, two-tier framework to replace the complicated and increasingly unworkable criteria now used to protect different types of information.

The committee has recommended that the prevalent approach to classification be reversed: Rather than assuming that information should be classified, the burden should be on showing the need for secrecy.

The committee's proposal would drop the "confidential" classification -- currently the lowest level assigned to secrets -- as recommended nearly thirty years ago by the Special Commission on Government Security.

At the second level of classification, the committee recommends special protective measures for a much smaller universe of data, based on a full analysis that assesses the risks.

-7-

And, the committee states that special protective measures should be imposed "only where necessary" and should not be "diluted by applying them too widely."

Streamlining the classification system should also make it possible to conduct independent audits of who has access to critical information, as a way to enforce the need-to-know principle.

Fourth, and even more important that the standards for classification, is the committee's recommendation that procedures be required for all authorized disclosures of legitimate secrets.

The Senate Intelligence Committee tries to follow two basic rules:

First, all media contact with staff are supposed to be forwarded to the committee press officer. And second, all statements by committee members or the committee spokesman should be fully on the record, so there is clear-cut accountability. We are also considering a more detailed code of conduct that may become part of the employment agreement signed by committee staff.

As far as we can tell, the executive branch does not have or enforce this kind of system. Yet, the practice of non-attributable background statements, often drawing on classified information, is pervasive.

Such statements are virtually indistinguishable from unauthorized leaks. They divert the overworked investigators of leaks from the cases in which administrative discipline, dismissal, or legal action is possible. And, they reinforce the climate of cynicism that leads to leaks and counterleaks.

Senior officials who authorize disclosures of classified information on background, without permitting attribution to the source, gain two advantages that undermine an effective information security system. First, they can conceal their responsibility for disclosure, just as the leaker does. Second, they can avoid giving the originating agency a chance to argue against disclosure and explain the harm it would do. If the same information disclosed "on background" were contained in a press release, it would have to be formally declassified.

In practice, however, classified information authorized for disclosure on background technically remains classified. There may well be valid reasons for retaining a "background" briefing classified character. But any serious effort to address the problem of leaks clearly must confront this practice and bring it under control.

Therefore, the committee recommends that the president require, by executive order, that agreed procedures be followed whenever any official authorizes disclosure of classified information to the news media. The procedure should require either that the information be declassified or that a record be maintained for purposes of accountability when authority is exercised to disclose information that remains declassified. The procedures should also require consulting the agency that originate the information and should designate the officials permitted to exercise this authority.

Fifth, on the polygraph, we are considering whether the time has come for Congress to give the Defense Department a long-term statutory framework to implement a tightly-controlled program for

-8-

polygraph examinations of employees in the most sensitive positions. When this proposal first surfaced in 1983, the committee supported the concept of a trial program to ensure that the Defense Department program is limited to questions directly related to counter-intelligence concerns, such as contacts with foreign agents; and the procedures prohibit adverse actions based solely on polygraph charts.

Sixth, is to guarantee accountability of superiors for ensuring that employees continue to meet security standards after their initial clearance.

One of the lessons of recent espionage cases is that initial background investigations for security clearance do very little to detect a Walker or Whitworth who turns sour after assignment to a sensitive job.

Seventh, it is clear that personnel security cannot stop with the clearance. It must be a continuing process of monitoring cleared people to ensure that they remain reliable.

This sounds intrusive, but it need not be. The best supervisor knows his subordinate's problem, be they financial, psychological, or behavioral. When superiors fail to exercise this duty and the result is a serious compromise of classified information, they -- as well as the culprit -- must be held to account and penalized appropriately.

Eighth, and finally, is the need to address concerns about the tremendous variety in standards and procedures among departments and agencies.

In 1983, the president ordered the Justice Department to head an interagency group to bring some order out of this chaos. They worked for a year, then waited almost two years for policy guidance from the NSC. That effort has now resumed, with a mandate to develop uniform, government-wide minimum standards for security background investigations.

At the very least, there should be an office responsible to the president for policy oversight of the personnel security system. We have such an office for the classification system, and it has come up with valuable improvements.

The resistance to this idea from entrenched security bureaucracies will be tremendous, because everybody wants to keep control of their security "turf." Nevertheless, the protection of national secrets is too important to be left entirely in their hands.

What I have tried to lay out here today is the notion that the problem of leaks is real and it stands as a threat to national security just as serious as spying against our government by a foreign power.

There are a number of factors contributing to the growing use of leaks which must be recognized in dealing with this problem, the most important of which is a pervasive attitude in some quarters in Washington that allows the long-term national interest to be subjugated to the opportunity for short-term political gain.

Fortunately, there is now a recognition, both within the Congress and the administration, that we must jointly develop a comprehensive and coherent program to address the full range of counter-intelligence and security issues. That recognition is one of the more positive outcomes of the "Year of the Spy" and "The Year of the Leak."

-9-

Both the Congress and administration must improve its system of accountability, define responsibilities more clearly, and establish internal mechanisms to prevent both leaks and espionage. Our shared responsibility is to come up with constructive and realistic measures that will begin to create a new commitment to the protection of legitimate national secrets.

National security is too important to demand of ourselves anything less.